Testimony of Deirdre Mulligan
Staff Counsel
Center for Democracy and Technology
before the
Senate Committee on Commerce, Science and Transportation
Subcommittee on Communications

September 23, 1998

I. Introduction

Good morning, I am Deirdre Mulligan, Staff Counsel at the Center for Democracy and Technology. The Center is pleased to participate in this hearing, at the request of the Subcommittee, on the Children's Online Privacy Protection Act (S. 2326) and the broader issue of protecting individual privacy in the online environment.

CDT is a non-profit, public interest organization dedicated to developing and implementing public policies to protect and advance civil liberties and democratic values on the Internet. One of our core goals is to enhance privacy protections for individuals in the development and use of new communications technologies.

It is our understanding that the Subcommittee is crafting their privacy agenda. My testimony this morning is intended to provide the Subcommittee with information on the current state-of-play on privacy, CDT's thoughts on what should be done to further protect individual privacy, and CDT's comments on The Children's Online Privacy Protection Act (S. 2326).

II. Summary

CDT believes that it is time for Congress and relevant stake holders to develop a bi-partisan national privacy policy for the Internet. While efforts at self-regulation continue, and are a necessary component of the electronic marketplace, legislation will speed the adoption of Fair Information Practices across the market, provide a level playing field, and ensure that bad actors are deterred. Toward this end, CDT has called for legislation enabling the Federal Trade Commission to develop rules to protect the privacy of both adults and children.

As Senators Bryan and McCain recognized in introducing The Children's Online Privacy Protection Act (S. 2326), the lack of privacy-protective business practices at Web sites designed for children is particularly troubling. Early this year the Federal Trade Commission and the White House reached the conclusion that legislation was

necessary to address the particular concerns surrounding children's privacy in the online environment. We strongly support the goal of The Children's Online Privacy Protection Act (S. 2326) and believe that the bill correctly places the crafting, implementation, and enforcement of the bills provisions at the Federal Trade Commission.

However, we believe that the bill as introduced will have a number of unintended consequences. We have expressed our concerns to Senator Bryan and will continue to work with him and the Subcommittee to address.

We strongly believe that appropriate legislation can protect privacy and aid electronic commerce by creating a level policy and practice playing field and a viable benchmark for oversight, enforcement, and redress. To accomplish the goals of protecting privacy and aiding electronic commerce, we believe that Congress should enact legislation enabling the Federal Trade Commission to craft baselines for protecting privacy during commercial interactions. The Children's Online Privacy Protection Act, if amended to address our concerns, would be a positive step in this direction. In addition, Congress should continue to explore and develop other legislative proposals to protect privacy, and explore the role of technology in protecting privacy and methods by which the government can promote the development of privacy-enhancing technologies.

We look forward to working with Senators Burns and Bryan and the rest of the Subcommittee to improve the Children's Online Privacy Protection Act (S. 2326) and to develop privacy protections for all Americans regardless of their age.

III. Why legislation is necessary

Recognizing that both individual company efforts and broader industry efforts to provide clear rules to protect privacy are growing, and are a necessary component of achieving privacy protection, we believe that a law providing the Federal Trade Commission the ability to set baseline rules to protect privacy and guide market

behavior will speed the adoption of privacy protective practices on the Internet. While private sector systems to protect privacy are likely to become more prevalent and robust, there are several reasons why Congress should act now:

- Individual privacy is under protected on the Internet

The Federal Trade Commission Report "Privacy Online: A Report to Congress" found that, despite increased pressure from the White House to develop meaningful self-regulation and growing public anxiety about privacy on the Internet, companies continue to collect personal information on the World Wide Web without providing even a minimum of consumer protection. The report looked only at whether Web sites provided users with notice about how their data was to be used; there was no discussion of whether the stated privacy policies provided adequate protection.

The report broke surveyed sites into six categories: (a) "comprehensive," general-interest sites; (b) health-related sites; (c) retail sites; (d) financial sites; (e) child-oriented sites; and (f) "most popular" sites. The report also discussed nine industry-specific self-regulatory guidelines disseminated by various trade associations.

The FTC surveyed 1,402 Web sites, taking 674 sites as a sample. The survey found that:

- 92% of the sites surveyed are collecting personally identifiable information

(although the type of sites surveyed may have artificially increased that percentage)
Of these sites almost all (98%) collected email address and 68% collected a name.
Two-thirds of the sites that collected a name and/or email address were collecting one or more types of information and almost half were collecting three or more types of information.
Despite the large number of sites collecting information, only 14% had some kind of disclosure of what they were doing with personal data.
At the FTC press conference announcing the report, Chairman Robert Pitofsky said that this figure included the most lenient interpretation of notice. By a stricter definition, only 2% had proper privacy notice. The most popular sites were significantly better at giving notice, with 61% giving some kind of disclosure and 44% providing comprehensive notice.

These figures show a clear lack of attention of industry to even the most basic of fair information practices. The gap between the most popular sites and the Internet as a whole is particularly striking, suggesting that the attention on the issue over the past three years has been mostly heard by a select number of big players online. The baselines set by the FTC need to be enforceable in order to create clear consequences for those that do not comply, expanding the discussion of privacy beyond the 111 most popular sites on the Net.

- **Children's privacy is under protected on the Internet**
  Particularly troubling to the FTC were the business practices of sites collecting information from children. While highlighting "the particular vulnerability of chidren," highlighting, the survey found that such sites were clearly not fulfilling the responsibilities associated with collecting such information from; individuals under 13 as outlined in previous FTC reports. The survey found that
- of children's sites were collecting personal information

only half had an information practice statement of any kind
fewer than a quarter had a privacy policy notice
only 7% of those sites collecting information notified parents; and,
only 23% even suggested that children speak to their parents before giving information.

The FTC's survey documented that business practices have not yet developed in a way that will protect children's privacy.

- **Electronic commerce is hindered by the distrust and anxiety of a public with deep-seated privacy concerns**

Numerous surveys have confirmed that Americans care deeply about their privacy. Several have tied concerns over the lack of privacy online to a reluctance to engage in electronic commerce.[1] A Business Week / Harris poll, published in the March 16 issue of Business Week, reveals that almost two-thirds of non-Internet users would be more likely to start using the Net if the privacy of their "personal information and communications would be protected." Privacy was the number one reason

[1] For background on privacy surveys, and CDT's analysis see http://www.cdt.org/privacy/survey/findings/bwbody.html
The Web site reviews: CDT's Survey '97; Business Week Poll '98; Georgia Institute of Technology '98; Privacy & American Business Poll '97; Cyber Dialogue '97; Truste/Boston Consulting Group '97; Narrowline '97; and, FamilyPC User Internet Study '98

individuals are choosing to stay off the Internet, coming in well ahead of cost, concerns with complicated technology, and concerns with unsolicited commercial email.

The rising tide of concern is evident in other results finding that over half of the respondents believe government should regulate the use and collection of personal information on the Internet, and that 65% are "very," and 15% "somewhat," concerned with using a credit card to make an online purchase. The results echo other recent privacy surveys that reveal users' privacy concerns are inhibiting use of the Internet.

- **The pro-active businesses and associations are actively engaged in efforts to protect privacy through self-regulation, however our current legal regime is more likely to punish them than those who have remained on the side-lines**

Recent efforts, such as BBB Online, the Children's Advertising Review Unit, the Online Privacy Alliance, and TrustE, to establish self-regulatory regimes to protect privacy indicate that some companies and trade associations are listening to consumer and policy makers concerns and responding. In the area of children's privacy, the Children's Advertising Review Unit's and the Online Privacy Alliance's guidelines, to a large extent, mirror the Children's Online Privacy Protection Act.

The active engagement of a portion of the responsible business community is often a necessary precursor to successful and effective legislative efforts. Their work can provide information, from the perspective of the business community, to legislators about the practicality and feasibility of particular rules. While the companies who have chosen to self-regulate are responding to consumers concerns, they run the risk of catching the Federal Trade Commission's eye if they inadvertently, or advertently, fail to live up to promises they make to consumers. Unfortunately, in today's environment, the cost of being responsible may be higher than the cost of waiting to see if public and policy-maker concern blow over.

- **Many businesses have yet to join the privacy movement, and the disincentives of our current legal regime encourage them not to act**

  Many companies have yet to take basic steps to protect privacy * such as providing visitors with notice of their information practices. As the FTC survey documented privacy policies are scarce on the World Wide Web. This may in part be do to a perverse incentive created by the FTC's enabling statute, which gives it more leeway to investigate those who make affirmative statements than those who fail to tell consumers how they are handling personal data.[2]

- **Self-regulation alone will not provide comprehensive privacy protections.**

  While self-regulation is a necessary part of any effective privacy regime on the global Internet, structural flaws in a purely self-regulatory system and specific difficulties that arise from the nature of the Internet suggest that self-regulation alone will result in incomplete protection. The four primary shortcomings of industry self-regulation in the privacy area have been: 1) the failure to incorporate core elements of fair information practice into substantive guidelines; 2) the lack of oversight and enforcement; 3) the absence of legal redress to harmed individuals; and, 4) the inability to set enforceable limits on government access to personal information.[3] Self-regulatory efforts to provide privacy protections on the Internet, to date, continue to exhibit these structural flaws.[4] These flaws are perhaps most

---

[2] See, Leonard Porter, 88 F.T.C. 546, 626, n.5 (1976). Commission was unwilling, absent extrinsic testimony evidence, to infer that an omission was deceptive); but see, e.g., Beneficial Corp., 86 F.T.C. 119 (1975), aff'd in part and rev'd in part on other grounds, 542 F.2d 611 (3d Cir. 1976), cert. denied, 430 U.S. 983 (1977) (deceptive to fail to disclose to consumers that information they provided to tax preparer would be used to solicit loans); Equifax, Inc., 96 F.T.C. 844 (1980), rev'd on other grounds, 678 F.2d 1047 (11th Cir. 1982) (deceptive to represent, inaccurately, that medical information would be released only to insurance companies); H&R Block, Inc., 80 F.T.C. 304 (1972) (consent), modified, 100 F.T.C. 523 (1982) (deceptive for tax preparer to fail to disclose use of tax information for purposes other than tax preparation).

[3] It is worth noting that advocates have voiced similar concern with the lack of effective oversight and enforcement provisions in existing legislative privacy solutions, which often lack private rights of action, significant penalties, and/or require the individual to show actual harm or damages to seek redress.

[4] For a full discussion of the limits of self regulation see, Testimony of Deirdre Mulligan Staff Counsel Center for Democracy and Technology before the House Committee on Commerce Subcommittee

troubling when contemplating children's privacy. In addition, the inability of young children to comprehend and consent to the collection and use of personal information; the need for parental involvement in children's online activities involving personal information; and, the potential risk posed by the public posting of information that facilitates contact (both online and offline) with a child, all suggest that government should move quickly to protect children's privacy. Building upon the work by non-profits and the private sector, the Children's Online Privacy Protection Act (if amended to address our concerns) could create an appropriate baseline of protection.

An added layer of difficult is posed by the complexity of implementing policy in a global, networked environment like the Internet. The diversity and multiplicity of players, the ease of crossing national borders, and the lack of centralized control mechanisms create challenges to those seeking to regulate activities on the Internet. The complexity of implementing policy in this global and distributed environment suggests that rather than relying on a single tool to implement policy, we should use the strengths of each in combination. This suggests that self-regulation, regulation and technology each must play a role in protecting privacy.

If Congress acts soon it can protect privacy, build upon and improve the ongoing activities in the private sector, establish a level playing field, and create a structure for oversight and enforcement of privacy practices on the Internet. Failure to act will result in continuing consumer distrust of the Internet, inadequate attention to individual privacy in the market place, and a legal framework[5] that in some instances actually

---

Telecommunications, Trade, and Consumer Protection, July 21, 1998.

[5] As Ori Lev, an F.T.C. official involved in Internet enforcement said, "There's now a perverse, reverse incentive. If you don't post a privacy policy, we can't go after you." David Medine said, "clearly there are a lot of corporate lawyers advising their Web clients not to do anything now" -- not to post a privacy statement or anything else. F.T.C. 'Losing Patience' With Business on Web Privacy," J. Brinkley , NYT, September 21, 1998.
The Federal Trade Commission's jurisdiction over deception generally comes into play where a company has inaccurately stated its information practices to consumers. Therefore, those who make no statements about how the handle data are less likely than those who inform consumers of data use to be

punishes those moving in the right direction[6] while creating no incentive for self-regulatory activities. It is clear to us that a more comprehensive and vigorous approach is required. However, we must also recognize that legislation will not on its own provide complete privacy protection. Privacy protection must build upon the strengths of existing efforts * self-regulatory and technical -- but fold them into a comprehensive system of enforceable privacy protections.

I V. Recommended legislative proposals to protect individual privacy including children's privacy

It is time to develop and move a national privacy policy forward. Such a policy must provide for the adoption and implementation of substantive policies that protect privacy throughout the private sector, the creation of legally enforceable privacy rights for individuals, the establishment of a national infrastructure to develop and oversee privacy policy, and support for privacy-enhancing technologies.

At this time, legislation is needed to accomplish two of these goals: the adoption and implementation of privacy policies in the private sector and the creation of legally enforceable privacy rights for individuals.

A. Privacy rules for the private sector

Over the past three years, the FTC has accumulated the knowledge and expertise necessary to set comprehensive guidelines for privacy online and in electronic commerce. However, the FTC has indicated that it do not believe it has the authority to affirmatively establish baselines in this area. The FTC's authority over privacy should be clarified and it should be explicitly given authority to establish baselines to protect

---

prosecuted. While the FTC's legal framework is likely to discourage self-regulatory activities, the FTC, the Department of Commerce and the White House have actively encouraged and prodded industry to take steps to protect privacy or be subject to legislation.

[6] The recent Geocities settlement offers an example of the problem. Geocities was found to be in violation of their privacy policy. Had they not posted a privacy policy it seems unlikely that the FTC would have sought them out for action.

the privacy of personal information based on the Code of Fair Information Practices.[7] Specifically the FTC should be directed to stablish baselines that require companies to:

- provide individuals with clear and conspicuous notice of information practices (including the data collected, its use, its disclosure and the items enumerated below); state the purposes for which personal data are collected at or before the time it is collected;
limit the collection of information to that which is necessary and relevant to the transaction and ensure that whenever possible anonymity be protected;
ensure that personal information is accurate and complete, is kept up-to-date, and is destroyed when it is no longer required;
gain the informed consent of the individual prior to using or disclosing personal information for purposes not related to the stated purpose;
provide consumers with access and correction rights to data about them; and
establish appropriate procedures and technical measures to safeguard personal information.

B. Web sites targeted at children and sites that knowingly collect information from children under 13

In the area of children under 13 years of age, the FTC should be directed to establish specific rules that address the inability of young children to comprehend and consent to the collection and use of personal information; the need for parental involvement in children's online activities involving personal information; the potential risk to children posed by the public posting of information that facilitates contact (both online and offline) with a child; and the need to ensure that business practices and privacy protections do not inappropriately interfere with children's ability to access information and receive information that they have requested and the benefits of interactivity.

[7] Such rules should be based on The Fair Information Practices developed by the Department of Health, Education and Welfare in 1973: 1. There must be no personal data record-keeping systems whose very existence is secret; 2. There must be a way for an individual to find out what information is in his or her file and how the information is being used; 3. There must be a way for an individual to correct information in his or her records; 4. Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and 5. There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers and the Rights of Citizens, U.S. Dept. of Health, Education & Welfare.

The Current Language of S.2326 and Its Unintended Consequences

While CDT strongly support the goal of the Children's Online Privacy Protection Act and believe that it appropriately charges the FTC with developing rules through a public process, and overseeing and enforcing the provisions of the Act, we believe that the bill as introduced will have a number of unintended consequences. We have worked with Senator Bryan's staff to address these concerns and believe that we can protect children's privacy, ensure children's First Amendment rights to access information are protected, and preserve the interactivity of children's online experience.

The Children's Online Privacy Protection Act of 1998 may unintentionally interfere with teenagers ability to access information and enjoy the interactivity of the Internet. As applied to teenagers the provisions that: 1) require parental notification every time a teenager provides an email address to a Web site that engages in commerce (including for-profit and non-profit Web sites); and, 2) create a parental right to access all information that a teenager has shared with a Web site that engages in commerce, have the potential to chill protected First Amendment activities and undermine rather than enhance teenagers privacy. In addition, we believe that requiring parental consent for email interactions between children and Web sites will prove cumbersome and interfere with children's ability to ask questions and access information. This is particularly true where children's access to the World Wide Web is through the school, library or other public institution.

Unintended Consequences of S. 2326

- Interfering with teenagers ability to access information and enjoy the interactivity of the Internet.

As applied to teenagers the provisions that: 1) require parental notification every time a teenager provides an email address to a Web site engaged in commerce; and, 2) create a parental right to access all information that a teenager has shared with a Web site that engages in commerce have the potential to chill protected First Amendment activities and undermine rather than enhance teenagers privacy.

- Interfering with teenagers access to information

Under the bill each time a 15 year old signs-up to receive information through email his or her parent would be notified. For example if a 15 year old visits a site, whether a bookstore or a women's health clinic where material is made available for sale and requests information about purchasing a particular book or merely inquires about books on a particular subject (abuse, religion) using their email address the teenager's parent would be notified. This may chill older minors in pursuit of information

- Creating a Parental right of access

In addition, the bill gives parents the right to access information about their teenager maintained by Web sites that engage in commerce. This would include information a teenager provided to a health related web site or through a questionnaire. The establishment of a parental right to access all personal information about a teenager may intrude on older minors' privacy, rather than protect. While the goal may be to put teeth into the Act by giving parents legal authority to see information on their children collected by others, in some instances teenagers may be divulging or seeking information they don't want their parents to know about. The detailed transactional data generated by use of the World Wide Web could reveal not just what a teen has purchased but every page visited at a site. This provision may authorize a second intrusion on teen's privacy by mandating parental access to potentially sensitive data. We agree that parents have an important role in protecting their teenager's privacy, however the bill's emphasis on parental access may overlook older minors' interests.

- Interfere with younger children's ability to access information online

As crafted the bill would limit children's ability to request information from a Web site (have a question answered, a newsletter delivered) via email without their parent's consent. The Internet allows information to be exchanged in a variety of ways. Some information is posted at Web sites for all to see, others is tailored to the individual's request * through search engines, the capability to request information through email, etc. If children may not request information through email, unless they obtain their

parent's consent, they may be shut off from this aspect. At the least, this provision may impede timely access to information, and in non-home settings such as schools and libraries prove particularly burdensome. Requiring parent's to act every time a child wants to receive information through email may place a burden on parents without much cause. If an email address is being used solely for the purpose of answering a child's question and will not be maintained or used for other purposes, it may be that parents need not be involved. We can develop a method that protects privacy but preserves interactivity * this should be our goal.

Suggested language changes to S. 2326

While we have communicated many changes to the staff, our major concerns can be addressed through the following changes:

- The definition of child should be changed to "under 13"[8]

The definition of commercial Web sites should clearly exclude non-profits
The target of the bill should be "Web sites targeted to children" and those "who know they are dealing with a child" (i.e. they collect information about age)
Allow children to ask for and receive information through email without parental involvement, where a Web site is bound not to use the email for any purpose other than to respond to the child's request
Provide for a process to examine the "verifiable parental consent" requirement, this is particularly important in non-home settings (schools, libraries, and other public institutions) where parental consent may unduly interfere with timely access to information

Protecting children's privacy and safety online is critical. The ongoing collection of personally identifiable information from children undermines children's privacy and is likely to scare parents into keeping their children off the Internet. As we ask our children not to disclose information about themselves * and as a society teach children to safeguard information about themselves and their families * in the real world, we must teach our children not to disclose their personal information to strangers in Cyberspace. The business community should not entice children into disclosing

[8] We are working with the Subcommittee to craft privacy protections for older minors that will respect their privacy and assure their First Amendment interests are protected.

information without their parent's knowledge and consent.

There is clear indication that rules must be set to protect children. A Federal Trade Commission survey of the World Wide Web found that many Web sites targeted at children were asking them for personal information. While recent industry efforts have begun to address this problem, as the FTC recently stated, we need rules to limit bad behavior and create a safe online environment. We hope that the committee will be able to balance all of the necessary concerns to address these problems,

C. Limits on use and disclosure of personal information by Web sites and Internet service providers

In addition, to ensure that personal information collected by Web sites and Internet service providers is protected from disclosure, and that government access to personal information collected and stored at Web sites is limited, the Electronic Communications Privacy Act (18 U.S.C. 2703) should be amended to:

- clearly cover World Wide Web sites; and

require consent (or parental consent where appropriate) prior to the disclosure of personally identifiable information to individuals or entities (other than government entities whose access to such information is already limited by ECPA).

V. Technology and privacy

In addition to crafting federal rules to protect privacy and encouraging private sector efforts at self-regulation, we must look to technologies that protect privacy. Such technologies can provide protection across the global and decentralized environment of the Internet where law or self-regulation alone may fail. Technology can provide a shield around the individual's actions, communications and identity, providing confidentiality, pseudonymity or anonymity. It can also serve as a mediator or facilitator capable of expressing and monitoring data practices and policies.[9]

[9] For example, audit trails that record the access and use of personal data by employees within an institution can assist in the oversight and enforcement of the institution's privacy policy.

There is growing evidence that the rapid decrease in cost and expertise needed to develop and use information technology coupled with the decentralized nature of the global network can be harnessed to significantly alter technology's traditional relationship to privacy. _A number of technologies have been put forward for protecting or enhancing privacy in networked environments. They vary from tools that provide near anonymity to those that seek to provide openness about data practices and foster informed decisions by individuals. The technologies differ in their ability to respond to and support the varied privacy concerns that arise in relationships, interactions and roles.

The World Wide Web Consortium's (W3C) Platform for Privacy Preferences (P3P) is a technical effort to provide a framework for implementing fair information practice principles on the Internet. The P3P effort attempts to leverage the unique characteristics of the Internet -- interactivity, real-time communication, and capacity to facilitate and support end-user decisions -- to facilitate privacy protection. The goal of the P3P project is to provide a common framework upon which various privacy policies and laws can be expressed, communicated, and complied with. P3P in conjunction with privacy protective business practices could greatly facilitate the protection of privacy on the World Wide Web and enable individuals to make informed decisions about the use of their personal information.

The Platform for Privacy Preferences provides a simple communication tool and language for the expression of data practices. In addition, the Platform for Privacy Preferences allows individuals to consider the data practices of an entity before interacting with it. Openness about data practices is likely to enhance the individual's ability to make choices that protect privacy and assist with the implementation of national and international policies.

The privacy "language" recently released by the W3C's Platform for Privacy

Preferences Vocabulary Working Group is intended to be descriptive, as opposed to normative. It allows various statements of information practice, thereby supporting various policies and legal regimes. As it is intended for global use, the language was crafted with attention to existing fair information practice principles as reflected in national laws and self-regulatory codes. While it has been critiqued for being both over- and under-inclusive, the vocabulary is a first attempt to provide a language for privacy practices on the Web.

P3P does not establish preset limits on the collection of personal information, however it promotes the ability of the individual, or those acting on their behalf, to set their own limits on the collection of information by others. It may be particularly useful in assisting parent's with setting limits on the information their children provide to Web sites.

The development of technological tools that enhance privacy should be promoted. Tools that facilitate anonymous interactions and those that allow individuals to control the flow of personal information once revealed are important to the protection of privacy in the online environment. Technology can be uniquely responsive to some of the obstacles the Internet poses to traditional methods of policy implementation. Many can be independently deployed by the individual and require no reliance on, or agreement with, the government or other party. They may provide protection in environments that lack legal or other policy protections for privacy, lessening concerns about citizens' interactions with entities outside national borders. They may also provide protection that exceeds that available under existing law. In addition, while they may not answer the normative question, "What is the appropriate policy?" the existence of technologies that support data privacy will force decisions about data collection and use into stronger relief.

The rise of technologies that empower individuals to affirmatively control personal information on international networks presents an opportunity to fundamentally shift the

balance of power between the individual and those seeking information. However, they must be viewed within the larger context of other efforts to produce cohesive privacy protections in the online environment. Currently US encryption policy is interfering with the availability of technical tools that protect privacy. Congress should seek to increase the availability of encryption and promote the development of other privacy-enhancing technologies.

V. Conclusion

Privacy protections must keep pace with changes in technology and society's use of technology. As we consider privacy in the changing communications environment we must question past assumptions and the legal distinctions based upon them. More importantly, we must ask whether they provide protections reflective of our commitment to individual privacy autonomy, dignity, and freedom. Privacy protection in the electronic commerce environment will best be achieved through a combination of legislation, self-regulation and technology.

Establish limits on the disclosure and use of personal information by private entities. Both the Federal Trade Commission and the Department of Commerce are engaged in initiatives designed to promote "fair information practice principles" in the online environment. We are encouraged that Congress is exploring protections for individual privacy during private sector activities. In considering this issue we recommend that Congress: 1) authorize the Federal Trade Commission to establish baselines for protecting privacy, including children's privacy grounded in the Code of Fair Information Practices; 2) work to improve and pass the Children's Online Protection Act (S. 2326) with suggested changes; and, 3) amend the Electronic Communications Privacy Act to clarify limits on government access to personal information and limit disclosures to third-parties.

Encourage the development and implementation of technologies that support privacy on global information networks. Technological mechanisms for protecting

privacy are critically important on the Internet and other global medium. Developing meaningful privacy protections in the online environment requires us to realize that our laws and Constitutional protections may not follow our citizens, their communications, or their data as it travels through distant lands. Technology can provide protections regardless of the legal environment.

Collaborate with other governments, the public interest community, and the business community to develop global solutions for the decentralized network communications environment.

Traditional top-down methods of implementing policy and controlling behavior, be they international agreements, national legislation, or sectoral codes of conduct enforced by the private sector, offer incomplete responses to the privacy issues arising on the global information infrastructure. Implementing privacy policy in the decentralized, global, and borderless environs of international networks raises difficult questions of effectiveness and enforcement. The US should work with all parties -- other governments, international bodies, and the public interest and for-profit communities to build consensus on appropriate policy. Providing a seamless web of privacy protection to individuals' data and communications as it flows along this international network may require new tools -- legal, policy, technical, and self-regulatory -- for implementing policy. The US should actively participate in their crafting.

Thank you for the opportunity to participate in this important discussion about protecting privacy in the online environment.